UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/534,855	05/13/2005	Michel Mahieu	28944/40154	9106

29471 7590 10/21/2009

MCCRACKEN & FRANK LLP
311 S. WACKER DRIVE
SUITE 2500
CHICAGO, IL 60606

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
10/21/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/534,855	MAHIEU, MICHEL	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 July 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *45-85* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *45-85* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/534,855 is presented for examination by the examiner. The amendments filed 7/6/09 have been entered. Claims 45-85 are pending.

Response to Amendment

Claim Rejections - 35 USC § 101

The claim amendments are sufficient in overcoming the previous 101 rejection.

Claim Rejections - 35 USC § 112

The claim amendments are sufficient in overcoming the previous 101 rejection.

Response to Arguments

Applicant's arguments filed 7/06/09 have been fully considered but they are not persuasive. The following interpretation of the prior art is solely based on the current set of claims and arguments submitted by the Applicant. It is not the only possible interpretation of the prior art and may be altered when/if the claims and/or arguments change.

Applicant alleges that the combination of Sung and Apostal fail to teach that the state of each component corresponds to a security status in the context of attacks launched against the system. Examiner respectfully disagrees with this allegation.

Sung discloses a system which is able to model and simulate attacks on a system. Sung teaches that the simulation results of each component of the system can be analyzed and evaluated with respect to the security policies of the network (pg. 328). If the result of the cyber attack can be deduced from the simulation results, there must inherently be some type of state assigned to each component that would yield some indication of the attack's result. Apostal's Checkmate Engine allows clients to submit attacks, view the state of nodes, and view the alarms that have been triggered on any node (pg. 218). This clearly teaches a sound state preceding an unsound state, the unsound state being equivalent to an alarm from the node. Furthermore, Apostal teaches evaluating the attack to exploit vulnerabilities and applying the effect of attack to the modeled node, which includes changing the state of said node (pg. 220). Apostal's results are more detailed and yield more specific results about a particular node than results of Sung's simulator. The claims would have been obvious because one of ordinary skill in the art could combine known methods which produce predictable results. Combining the nodal changes of Apostal produces a more detailed analysis of the effects of the simulated network attack.

With respect to the allegation Sung fails to teach the first and second behavioral rules, this argument is moot because merely stating that a reference does not teach a feature because said reference is unclear is not persuasive. Applicant has not provided

evidence of why he believes the Sung reference is different from the claimed subject matter.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 45-48, 52, 53, 55, and 83 are rejected under 35 U.S.C. 103(a) as being unpatentable over NPL "Network Security Modeling and Cyber Attack Simulation Methodology" to Sung et al. published 7/11/01, hereinafter Sung in view of NPL "Checkmate Network Security Modeling" to Apostal D et al. published 6/12/01, hereinafter Apostal.

With respect to claim 45, Sung teaches the limitation of a "modeling phase, comprising a specification of an architecture of the information system with a graphical representation of a set of components of the information system and relations between said set of components, each component being associated with at least one state initialized with a sound value, the relations between two determined components comprising propagation relations able to convey attacks, and a specification of first and

second sets of behavioral rules, the first set of behavioral rules from the standpoint of the operation of the system [framework and underlying modeled network functionality] and the second set of behavioral rules from the standpoint of security [how the nodes respond to attacks], associated with the components of the system, each behavioral rule comprising one or more predicates and/or one or more actions" (page 321, lines 10-18) as the network security modeling and cyber attack simulation employing the advanced modeling and simulation concepts that supports a hierarchical and modular modeling environment, which (page 323, lines 7-14) consists of a system entity structure (SES) and model base (MB). The SES represents the knowledge of decompositions, taxonomies, coupling specification and constraints. The model base contains models that are procedural in character, expressed in discrete event system specification formalism. Furthermore (page 325, lines 18-20) dynamics of the component models can be represented in various ways according to their respective state variables. Finally, Sung discloses the graphical representation (Fig. 8; page 331, lines 1-8) as SECUSIM system where users can set up initial conditions for simulation by using windows of each node. Sung teaches implementing the modeling phase and the simulation phase on a computer that includes a man/machine interface and an attacks/parries engine (Fig. 8, page 331).

In addition, Sung does not explicitly disclose the limitations that each initialized state corresponds to a security status of each component in the context of attacks launched against the information system" and that "a successful attack causing a state of a component to pass to an unsound value".

On the other hand, Apostal teaches the state of a node correspond to an attack (pages 218, and 220). Apostal also teaches a successful attack causing a state of a component to change to an unsound value [alarm; pg. 218 and 220].

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Apostal into the system of Sung to provide means for storing additional information about the network and its components. The claims would have been obvious because one of ordinary skill in the art could combine known methods which produce predictable results. Combining the nodal changes of Apostal produces a more detailed analysis of the effects of the simulated network attack.

With respect to claim 46, Sung teaches the limitation of "a name [service type] being associated with each component one or more adjectives [execution of each phrase] may also be associated with said component, which adjectives make it possible to designate said component without naming it" (pg. 326, Fig 5).

With respect to claim 47, Sung teaches the limitation of "determined states are associated with each component of the information system, each state being able to take a sound value [phases] and one or more unsound values" (pg. 326, Fig 5) as the server allows client to view the state of nodes and resources and (pg 331).

With respect to claim 48, Sung teaches the limitation of "certain at least of said states pertain respectively to the activity, the confidentiality, the integrity and/or the availability of the component with which they are associated" (pg 326, Fig. 5).

With respect to claim 52, Sung teaches the limitation of "the relations between any two determined components comprise service relations making it possible to designate a component on the basis of another component" (page 325, lines 17-20) as network component model comprises various services such as Telnet, Email, Ftp, Web, and Packet Filtering. The dynamics of these component models can be represented in various ways according to their respective stated variables.

With respect to claim 53, Sung teaches the limitation of "the behavioral rules comprise rules for propagating attacks, these rules being for example implemented in components which are vectors of attacks, and rules for absorbing attacks, these rules being for example implemented in components which are the target of attacks" (page 327, lines 10-12) as the attacker model outputs a sequence of attacking commands according to its attacking scenarios.

With respect to claim 55, Apostal teaches the limitation of "at the end of the modeling phase, the construction of a local routing table, making it possible to direct an attack from a start component to a finish component" (page 216, right column, lines 26-

29) as map table that holds locations and size information for elements (nodes and network segments) that are drawn on the network map.

With respect to independent claim 83, it is rejected in view of the same reasons as stated in the rejection of independent claim 45.

Claims 49-51 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sung et al. and Apostal D as applied to claim 45, and further in view of Ritchey at al. "Using model checking to analyze vulnerabilities." Proceedings of the 2000 IEEE Symposium on Security and Privacy. 05/14-17/2000, pages 156-165.

With respect to claim 49, it is noted that neither Sung nor Apostal explicitly teach the limitation of "an alleged name may be associated with any determined component, in particular in the case where said determined component is a usurper."

On the other hand, Ritchey teaches the abovementioned limitation (page 162, left column, lines 43-46) as Hostid is sequentially assigned to each host and is used to index into the row and column of the connectivity matrix. The attacker is assigned hosted one, so the Hostid numbering starts at two.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Ritchey into the system of Sung and Apostal to provide a straight-forward method of determining whether a host can communicate with another host.

With respect to claim 50, Ritchey teaches the limitation of "a link to another component may be associated with any determined component, in particular in the case where said determined component is usurped and where said other component is a usurper" (page 162, right column, lines 36-41) as the connectivity matrix is used to determine whether a host can communicate with another host. The host ids for the source and destination hosts are used to index into the row and column of the matrix to determine if communication is possible.

With respect to claim 51, Ritchey teaches the limitation of "the propagation relations are bidirectional relations able to convey attacks in both directions" (page 160, right column, lines 34-40) as in our SMV example we have modeled connectivity with a Boolean matrix that has the distinct disadvantage of not allowing our model to describe partial connectivity. This choice was made to simplify the example. It would be an easy task to add a richer connectivity description to our method that includes common network connectivity details such as port numbers.

With respect to claim 54, it is noted that neither Sung nor Apostal explicitly teach the limitation of "the behavioral rules comprise binary rules, for example Boolean logic conditions giving a value of type yes/no, and/or functional rules, for example logic conditions involving a routing action (for a propagation rule) or contagion action (for an absorption rule)."

On the other hand, Ritchey teaches the abovementioned limitation (page 163, left column, lines 11-13) as an exploit is described by a case statement that determines whether all of the prerequisites for the exploit have been met.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Ritchey into the system of Sung and Apostal to provide a better way to determine the severity and probability of the system's exploits.

Claims 56, 57, 59-61, 67-69, 71-73, 84, and 85 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sung et al. and Apostal as applied to claim 55 above, and further in view of Gupta et al. (US 7,289,456 B2).

It is noted that neither Sung nor Apostal teach the limitation of "the local routing table is generated automatically according to the principle of the shortest path between the start component and the finish component."

On the other hand, Gupta teaches the abovementioned limitation (column 13, lines 47-59) as the routing engine will determine multiple paths between the two routing nodes. Specifically, the routing engine may determine a shortest path and one or more alternate shortest paths (i.e., a second, third, etc. alternate shortest path), using for example, the Dijkstra Algorithm. The former determination can be performed by first determining a shortest path to the destination node and by then determining alternate shortest paths by determining a shortest path to each of the destination node's neighboring routing nodes.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Gupta into the system of Sung and Apostal to provide more efficient network model.

With respect to claim 57, Apostal teaches the limitation of "the attacks simulation step comprises the updating of the state of a component of the system altered by a successful attack" (page 220, lines 2-6) as the Checkmate server evaluates the attack action and applies the effects of that action to the model network. The possible effects of an attack action include changing the state of a node or protocol.

With respect to claims 59 and 60, Apostal teaches the limitations of "the attacks comprise elementary attacks corresponding to unsound state values" and "the attacks further comprise a special usurping attack" (page 219, left column, lines 9-13) as an attacker can send commands that simulate requests for service functionality, that change services or nodes, and that exploit vulnerabilities.

With respect to claim 61, Apostal teaches the limitation of "an attack is defined, in particular, by a type of attack, a type of protocol, and attack path elements" (page 218, left column, line 20 – right column, line 1) as each role has associated with it a number of characteristics including: a set of nodes to attack, a set of nodes to defend, a set of mission objectives, a set of initial resources, and a level of programming ability.

With respect to claim 67, Sung teaches the limitation of "the attacks are defined in a language using the same words as a language in which the behavioral rules are defined" (page 325, lines 5-8) as the experimental frame concept may be suitably utilized to couple with a given network model, generates input external events (cyber attack commands), monitor its running (consequences), and process its output (vulnerability).

With respect to claim 68, Sung teaches the limitation of "the modeling phase and/or the simulation phase are implemented by a user by means of a man/machine interface comprising a multi-view functionality, wherein a graphical representation of the system is presented to the user as several views" (page 331, lines 1-8) as a network security simulation system where users can set up initial conditions for simulation by using windows of each node. The can also try to test various cases by attaching attacker and analyzer to any particular node. Procedures of simulation can be checked by the packet-based animation and more detailed procedures can be checked through given windows.

With respect to claim 69, it is rejected in view of the same reasons as stated in the rejection of claim 68.

With respect to claim 71, it is noted that neither of Sung, Apostal, and Gupta teach the limitation of "the behavioral rules for the components belonging to a view do not call by name upon components belonging to another view."

On the other hand, examiner takes the official notice that isolation of the elements is in the network system is not a novel concept and therefore, it would have been obvious to one of the ordinary skill in the art to provide no other ways for components to reference each other, other than through the information defined in the routing table controlled by the administrator to improve the security of the system.

With respect to claims 72 and 73, they are rejected in view of the same reasons as stated in the rejection of claim 68.

With respect to claims 84 and 85, they are rejected in view of the reasons stated in the rejection of claim 68.

Claim 58 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sung, Apostal, and Gupta et al. as applied to claim 57 above, and further in view of Dowd et al. (US 7,315,801 B1).

With respect to claim 58, it is noted that neither of Sung, Apostal, or Gupta teach the limitation of "the simulation phase furthermore comprises the building of a file or journal of the attacks, containing the log of the changes of the state of the components

consequent upon successful attacks, in particular to allow subsequent processing by a user."

On the other hand, Dowd teaches the abovementioned limitation (column 14, lines 11-13) as the security modeling system includes a log or a recorder which allows the system to play back the moves of an attacker or defender or both.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Dowd into the system of Sung, Apostal, and Gupta because the system logs would provide the ability for the administrator to examine data retroactively.

Claims 62-66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sung, Apostal, and Gupta et al. as applied to claim 61 above, and further in view of Cohen et al. (US 6,952,779 B1).

With respect to claim 62, it is noted that neither of Sung, Apostal, or Gupta explicitly teach the limitation of "the attack path elements comprise a start component, a finish component, a target component, and as appropriate one or more intermediate components."

On the other hand, Cohen teaches the abovementioned limitation (column 7, lines 1-2) as the system simulates attacks through the network topology from each start point to each end point.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Malan into the system of Sung, Apostal, and Gupta to provide a better security by quickly and robustly correlating the statistics collected from the network to reconstruct the path of the attack.

With respect to claim 63-66, Cohen teaches the limitations of " the list of components already traversed by an attack is saved in one or more upstream stacks", "the upstream stacks comprise a stack containing the exhaustive list of all the components traversed, designated by their real name", "wherein the upstream stacks comprise a stack containing the list of only those components traversed which are opaque, designated by their real name or, as appropriate, by their alleged name", and "the list of destination components of an attack is saved in at least one downstream stack" (column 7, lines 25-35) as the attack simulation commences from a specified attack starting point. The system then loops through a moving front-line algorithm by repeatedly evaluating the constraints for every state/graph node that has not yet been reached. The moving front-line algorithm continues adding edges to new graph nodes until no more states/graph nodes can be reached at which point the process terminates.

Claims 70 and 74-76 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sung, Apostal, and Gupta et al. as applied to claim 68 above, and further in view of Pitchaikani et al. (US 6,061,505).

With respect to claims 70, it is noted that neither of Sung, Apostal, and Gupta explicitly teach the limitation of "the function of interconnection between the components included in two distinct views is ensured only via the common component or the common components shared by the two views" (column 10, lines 48-54) as each view record of view records includes information about a given logical view, and is connected by a plurality of pointers to a plurality of view device records. Each view device record of view device records contains an index that indicates which device interface exists in a particular logical view. Furthermore, (column 11, line 7) to represent this relationship between various views, a plurality of pointers associates each view record of view records that represents a view having a subview with the view records in view records which represent the one or more subviews. Where subview can be a view of the station alone.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Pitchaikani into the system of Sung, Apostal, and Gupta to create a logical topology map of the network.

With respect to claims 74 and 75, it is rejected in view of the same reasons as stated in the rejection of claim 70.

With respect to claim 76, Pitchaikani teaches the limitation of "the modeling phase further comprises the specification of one or more basic metrics associated respectively with the components" (Table 5; column 11, line 53 – column 12, line 5) as

database includes TopoMonitor records, polling records, location records, describe records, ExtView Info records, AppSpecificinfo records, Mgmt Addr records, etc.

Claims 77-82 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sung, Apostal, Gupta et al., and Pitchaikani et al. (US 6,061,505) as applied to claim 76 above, and further in view of Swiler et al. (US 7,013,395 B1).

With respect to claim 77, Sung teaches the limitation of "the basic metrics comprise a metric of effectiveness of parries, a metric of effectiveness of detection of attacks, and/or a metric of the means of an attacker" (page 327, lines 19-22) as the analyzer model is designed to gather the statistics and analyze the performance index such as the vulnerability of each component on given network. For the simulation convenience, we have defined the component vulnerability as the number of successful attacks divided by the total number of attempted attacks.

In addition, Swiler further teaches the abovementioned limitation as (column 7, lines 7-11) as the attack template also contains an edge weight. When the template is instantiated, it returns a value that is the weight on the edge in the attack graph. The value may represent time for the attack to succeed, cost to the attacker, etc., depending on which metric the user chooses. Furthermore, (column 9, lines 56-64) each node in the graph contains information about what user privileges the attacker has obtained, extra vulnerabilities not implied by the privilege level, and the shortest distance from the start to the current node. Distance, in this case relates to the edge weight functions in

the attack templates and represents such considerations as estimated time, cost, degree of effort, and likelihood of detection of the attack.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Swiler into the system of Sung, Apostal, Gupta, and Pitchaikani to provide the extensive view of the attack paths and advantages gained by the attacker.

With respect to claims 78-82, they are rejected in view of the same reasons as stated in the rejection of claim 77.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431